ケーススタディ

# アトラシアン・ウィリアムズF1チーム、KeeperPAM®で特権システムへの重要なアクセスを安全に管理


## 背景

**アトラシアン・ウィリアムズF1チームは、1977年にサー・フランク・ウィリアムズとパトリック・ヘッドによって設立された、フォーミュラ1の中でも長い歴史を持つチームの一つです。英国オックスフォードシャー州グローブを拠点とし、これまでにコンストラクターズチャンピオンシップ9回、ドライバーズチャンピオンシップ7回を獲得するなど、F1史上でも屈指の実績を誇ります。卓越したエンジニアリング力と高い競争心で知られる同チームは、技術革新とパフォーマンスを重視し、最先端の技術やデータ分析を活用しながら、変化の激しいモータースポーツの世界で常にトップ争いを目指しています。**

**業種**
モータースポーツ

**従業員数**
1000人以上

**ソリューション**
KeeperPAM

## 課題

フォーミュラ1の世界では、機密性の高いパフォーマンスデータを守ることが、競争優位性を維持するうえで欠かせません。アトラシアン・ウィリアムズF1チームにとっての課題は、レースウィークエンドの高い緊張感の中で稼働する数百台のデバイスに加え、平常時の業務も含め、世界各地で働くスタッフによる特権アクセスをいかに安全に管理するかという点にあります。重要なシステムは複数の大陸にまたがり、さまざまなネットワーク環境で運用されています。そのため、最も価値の高い情報を確実に保護しながら、業務のスピードを落とすことなく、重要なデータの安全性を維持することが求められていました。

> **「現在では、サーキットで生み出される極めて機密性の高いデータを守るために、信頼できるパートナーの存在が不可欠です。」**
>
> **カルロス・サインツ | アトラシアン・ウィリアムズF1チーム F1ドライバー**

ウィリアムズは、シーズンを通じて20か国以上で活動しており、デバイスや認証情報は大陸を越えて常に移動しています。そのため、拠点やネットワーク、端末の種類に左右されることなく、どの環境でも有効に機能するセキュリティ対策が求められていました。本拠地にいる場合はもちろん、サーキットで一時的に構築されたネットワークに接続する場合でも、チーム全体を確実に保護できる体制が必要だったのです。

こうしたアクセス管理には、別の課題もありました。多数の社内部門や役割、システム、地域にまたがって認証情報を付与・削除する作業には、多くの工数と時間がかかっていました。

> **「通常、コンピューターは一つの建物内で使われますが、私たちのものは世界中を移動します。どこへ行っても、技術の安全性を確保し続けなければなりません。」**
>
> **ジェームズ・ボウルズ | アトラシアン・ウィリアムズF1チーム チーム代表**

## Keeperのソリューション

アトラシアン・ウィリアムズF1チームは、Keeper Securityと連携し、ゼロトラストおよびゼロ知識の考え方に基づく包括的な特権アクセス管理 (PAM) プラットフォームである**KeeperPAM**を導入しました。KeeperPAMの統合プラットフォームにより、スピード感のある業務環境と世界各地に分散したチームにおいて、特権アクセスを管理するために必要な可視性、セキュリティ、運用の柔軟性を確保できるようになりました。同チームでは、機密データを確実に保護しつつ、アクセス状況をきめ細かく把握できる、導入しやすいソリューションが求められていました。

**ロールベースの最小権限アクセス** – KeeperPAMのきめ細かな**ロールベースのアクセス制御 (RBAC)** により、技術・イノベーション推進部門の各メンバーは、自身の役割 (ロール) に必要な認証情報、システム、データのみにアクセスできます。権限を厳格に制限することで、内部不正のリスクを抑え、機密データへの不要なアクセスを最小限に抑えています。

**特権認証情報の安全な管理** – パスワードやパスキーといった特権認証情報は、Keeperの**ゼロ知識およびゼロトラストのセキュリティアーキテクチャ**のもとで安全に保管・管理されます。これにより、不適切な保存方法によるリスクを排除し、認証情報が平文で扱われることを防ぎます。チームが世界のどこで活動していても、重要なログイン情報を確実に保護できます。

> **「Keeperを使い始めると、多くの人が『これまで何が足りなかったのか』にすぐ気づきます。パスワードの入力に手間取ったり、情報をどう安全に共有するかで悩んだりする必要がなくなるからです。使いやすさのおかげで、すべての利用者において、セキュリティの向上と同時に生産性も大きく高まります。」**
>
> **- クレイグ・ルーリー | Keeper Security CTO兼共同創業者**

**パスワードレスアクセス** – 特権セッション管理の機能により、ウィリアムズのセキュリティ担当チームは、認証情報を開示することなく機密システムへのアクセスを付与できます。KeeperPAMを活用することで、特権操作をリアルタイムで監視・記録・監査でき、完全な可視性と管理性を確保できます。

**既存システムとのスムーズな連携** – KeeperPAMは、ウィリアムズのID管理基盤と**直接連携**し、特権アカウントの付与や削除を自動化します。これにより、メンバーの参加や離脱時にも、アクセス権限を即座かつ正確に反映でき、管理負荷を軽減するとともに、不要なアクセスが残るリスクを防ぎます。

**高水準のセキュリティ** - Keeperは、ゼロトラストおよびゼロ知識のセキュリティアーキテクチャを採用し、情報の保護とデータ漏えいリスクの低減に取り組んでいます。端末レベルでの楕円曲線暗号 (ECC) に加え、ボルト、フォルダ、レコードの各階層で**複数層の暗号化**を適用しています。さらに、多要素認証や生体認証、FIPS 140-3に準拠したAES 256ビット暗号とPBKDF2を組み合わせることで、堅牢なセキュリティ基盤を構築しています。また、Keeperは**SOC 2、ISO 27001、27017、27018に準拠**しており、これらの認証要件への対応を長年にわたり継続してきました。加えて、FedRAMPおよびGovRAMPの認可、PCI DSS認証、プライバシー分野におけるTrustArc認証も取得しています。

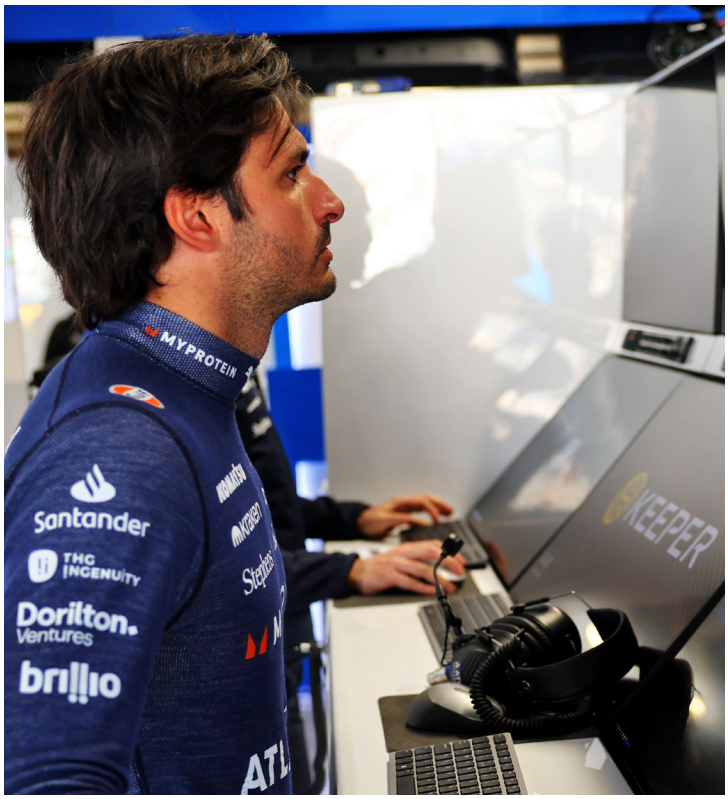
> **「これまで利用してきた他のツールと比べても、Keeperのオンボーディングははるかに迅速で、導入しやすいと感じました。」**
>
> **ハリー・ウィルソン | 元アトラシアン・ウィリアムズF1チーム情報セキュリティ責任者**

## 組織への影響

Keeperの導入により、アトラシアン・ウィリアムズF1チームにおける特権アクセスの管理と保護の在り方は大きく変わりました。現在では、最も高い権限を持つ利用者に対してもPAMポリシーを徹底し、ゼロ知識ボルトで認証情報を安全に管理するとともに、世界中どこからでも迅速かつ安全に接続できる環境を整えています。さらに、特権操作の監視やアクセス権限の変更が自動化されたことで、業務スピードと運用の確実性、そして管理性が一段と高まりました。

> **「私たちがパートナーシップにおいて重視しているのは、両ブランドが同じ目標に向かって協力し合える相乗効果があるかどうかです。その点で、Keeperとの関係には確かな手応えがあります。」**
>
> **ジェームズ・ボウルズ｜アトラシアン・ウィリアムズF1チーム チーム代表**

**特権アクセスのセキュリティと可視性を強化** – KeeperPAMは最小権限アクセスを徹底し、すべての認証情報を暗号化されたボルトで安全に管理します。さらに、SSH、RDP、VNC、データベース、ウェブブラウザセッションなど、あらゆるプロトコルに対応し、リモートセッション中の画面操作やキーボード操作を記録できます。これにより、ウィリアムズは特権操作の状況を的確に把握できるようになりました。





**認証情報管理の強化** – KeeperPAMの導入により、ウィリアムズではすべてのシステムで多要素認証 (MFA) を適用し、チーム全体でパスワード強度が基準を満たすよう徹底しています。また、利用者間でのパスワードの使い回しも早期に把握できるようになりました。Keeperの監査・レポート機能を活用することで、重複した認証情報の利用を排除し、潜在的なサイバー脅威に対しても高い安全性を維持しています。

**高い利用定着率とサポート対応の削減** – KeeperPAMは直感的に使える設計のため、組織全体でスムーズに定着しました。その結果、パスワードやアクセスに関するヘルプデスクへの問い合わせが減り、ITチームの負担軽減につながっています。また、KeeperPAMの**ドキュメントポータル**も、利用者が操作に慣れるうえで役立ちました。高い定着率により、管理者とエンドユーザーの双方にとって、日常業務がより円滑で安全なものになっています。

> **「サーキットで業務にあたるチームにとって、Keeperは使いやすさと高い安全性を両立してくれました。無理なく使える運用がそのまま安全性の向上につながり、結果として利用者も満足し、私自身も安心しています。」**
>
> **ハリー・ウィルソン｜元アトラシアン・ウィリアムズF1チーム 情報セキュリティ責任者**

**グローバルな業務運用への信頼性** – Keeperの活用により、ウィリアムズは世界中のどこにいても、ネットワークやデバイスの種類を問わず、安全に業務を行える体制を維持しています。サーキット現地や本拠地、次のレースへの移動中であっても、重要な情報を適切に保護しながら業務を継続できます。

# KeeperPAM

KeeperPAMは、サーバー、ウェブアプリケーション、データベース、ワークロードなどの重要なリソースへのアクセスを安全に管理する、次世代の特権アクセス管理(PAM)プラットフォームです。ゼロトラストおよびゼロ知識のセキュリティアーキテクチャを基盤としており、組織の規模を問わず、特権アカウントの保護、最小権限の徹底、リモートインフラの安全な運用、コンプライアンス要件への対応を支援します。高い操作性と導入のしやすさを備えている点も特長です。

Keeperは、企業規模を問わず直感的に使え、導入もしやすい設計となっています。KeeperPAMでは、ゼロトラスト型のゲートウェイサービスを通じて各環境へアクセスする仕組みを採用しており、ファイアウォールの設定変更やインバウンド通信の追加は不要です。そのため、複雑な構成を伴わずに、安全でスムーズなアクセスを実現できます。また、リモートセッション機能により、利用者がパスワードやSSHキーといった認証情報に直接触れることはありません。リソースへのアクセスは時間制限を設けることができ、アクセス終了後には認証情報が自動的にローテーションされます。これにより、認証情報を開示することなく、ジャストインタイム (JIT) での安全なアクセス管理が可能となります。

Keeperは、組織の規模を問わず利用できるよう設計されています。KeeperPAMでは、複数のクラウドプロバイダー、オンプレミスのワークロード、顧客環境にまたがるアクセス管理を、単一のユーザーインターフェース (UI) に集約しています。これにより、マルチクラウド環境全体を一元的に管理できます。

### KeeperPAMのビジネス活用事例

- すべての特権アカウントを管理・監視
- 認証情報を開示せずにジャストインタイム (JIT) アクセスを実現
- 直感的なUIで開発ツールをひとつのプラットフォームに集約
- クラウド、ハイブリッド、マルチクラウド環境を一元的に管理
- AIによる脅威検知と自動セッション終了に対応し、複数プロトコルのセッションを記録
- パスワードのローテーションを自動化
- すべてのシステムで多要素認証 (MFA) を適用
- ウェブまたはデスクトップアプリからスムーズに導入でき、SCIMによる自動プロビジョニングに対応

### Keeperで組織を保護

使いやすいプラットフォームでKeeperがどのように組織を保護できるのか、詳しく知りたい方は、営業チームまでお問い合わせください。無料トライアルや、お客様に合わせたデモをご案内します。

## Keeperについて

Keeper Securityは、150以上の国で幅広い企業や利用者を守る、急成長中のサイバーセキュリティソフトウェア企業です。ゼロ知識とゼロトラストを基盤とし、あらゆるIT環境に対応できるセキュリティの先駆けとして知られています。主力製品のKeeperPAM®は、AIを搭載したクラウドネイティブのプラットフォームであり、ユーザーやデバイス、インフラを包括的にサイバー攻撃から保護します。特権アクセス管理 (PAM) の分野では、ガートナー社の「Magic Quadrant (マジック・クアドラント)」において革新性が高く評価されました。Keeperではロールベースのポリシー、最小権限、ジャストインタイムアクセスを組み合わせることで、パスワードやパスキー、インフラのシークレット、リモート接続、エンドポイントを安全に管理しています。

**Keeperは、世界各地の企業や利用者から高い信頼を得ています。**

Cybersecurity Excellence Award
**特権アクセス管理**

Cyber Defense Magazine
**エディターズチョイス - 特権アクセス管理 (PAM)**

Newsweek
**No.1サイバーセキュリティプラットフォーム**

エンタープライズ・マネジメント・アソシエイツ
**KeeperPAM®、優れた製品力で高い評価を獲得**

**KeeperPAM®、Gartnerの2025年版Magic Quadrant™ (PAM部門) に選出**